Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Administrator Bezpieczeństwa Informacji w podmiotach leczniczych

Analizując wprowadzone w Polsce przepisy ustawy[1], a także planowane na 2016 rok regulacje UE dotyczące przetwarzania danych osobowych w UE wydaje się, że w przypadku podmiotów leczniczych i systemu informacyjnego opieki zdrowotnej w większości przypadków koniecznym będzie powołanie Administratora Bezpieczeństwa Informacji (ABI). W artykule przedstawiamy najważniejsze aspekty funkcjonowania ABI, wymagania stawiane przed ABI, konieczność rejestracji i obowiązki.

W polskim prawodawstwie zastosowano nazwę Administrator Bezpieczeństwa Informacji (ABI), natomiast w planowanym rozporządzeniu UE[2] stosuje się określenie inspektor ochrony danych.

Przewiduje się, że inspektor ochrony danych, który może być pracownikiem administratora danych i może pracować na pełny etat, powinien być w stanie niezależnie wykonywać swoje obowiązki i zadania oraz korzystać ze specjalnej ochrony przed odwołaniem z funkcji . Ostateczna odpowiedzialność powinna nadal spoczywać na kierownictwie danej organizacji.

Opinii inspektora ochrony danych należy zasięgnąć w szczególności przed zaprojektowaniem, zamówieniem, opracowaniem i ustanowieniem systemów automatycznego przetwarzania danych osobowych, aby zapewnić zgodność z zasadami ochrony prywatności już w fazie projektowania oraz domyślnej ochrony prywatności.

Jeśli administrator lub podmiot przetwarzający są organem lub podmiotem

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. 1997 nr 133 poz. 883
[2] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

publicznym, inspektor ochrony danych może być wyznaczony dla szeregu jego jednostek organizacyjnych, z uwzględnieniem struktury organizacyjnej organu lub podmiotu publicznego.

Wymagania i kwalifikacje ABI

W ustawodawstwie polskim określono także wymagania w stosunku do administratora bezpieczeństwa informacji, może nim być osoba, która:

- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
- nie była karana za umyślne przestępstwo[3].

Wyższe wymagania przewiduje rozporządzenie UE. Inspektor ochrony danych powinien mieć co najmniej następujące kwalifikacje:

- obszerną wiedzę na temat treści i stosowania prawa o ochronie danych, w tym na temat technicznych i organizacyjnych środków i procedur;
- znajomość wymogów technicznych odnoszących się do ochrony prywatności w fazie projektowania, do domyślnej ochrony prywatności oraz do bezpieczeństwa danych;
- wiedzę branżową odpowiadającą wielkości działalności administratora lub podmiotu przetwarzającego oraz poufnemu charakterowi danych, które mają być przetwarzane;
- umiejętność prowadzenia inspekcji, konsultacji, dokumentacji i analizowania plików dziennika; umiejętność współpracy z przedstawicielami pracowników.

Administrator danych powinien umożliwiać inspektorowi ochrony danych udział w zaawansowanych szkoleniach mających na celu utrzymanie poziomu specjalistycznej wiedzy niezbędnej do wykonywania jego obowiązków. Wyznaczenie do pełnienia funkcji inspektora ochrony danych nie musi wymagać pracy danego pracownika w pełnym wymiarze.[4]

[3] **Art. 36a.5** Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. **Dz.U. 1997 nr 133 poz. 883**

[4] 75a Poprawka 50 Wniosek dotyczący rozporządzenia Motyw 75 a (nowy) Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Zgodnie z przepisami ustawy o ochronie danych osobowych administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki - analogiczne jak ABI. Jest to istotne, gdy ABI przejściowo nie może realizować swoich zadań.

Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań.

Przepisy nie zakazują wykorzystywania wyspecjalizowanych podmiotów zewnętrznych do wykonywania zadań administratora bezpieczeństwa informacji .

Warunkiem koniecznym prawidłowego usytuowania w podmiocie leczniczym , jest zgłoszenie powołanego ABI w terminie 30 dni od powołania do rejestru prowadzonego przez GIODO. Sprecyzowano[5] jakie dane powinno zawierać zgłoszenie:

1) oznaczenie administratora danych (czyli podmiotu, który prowadzi rejestr danych osobowych),

2) dane ABI (imię i nazwisko; numer PESEL (lub innego dokumentu stwierdzającego tożsamość, gdy brak nr PESEL),

3) datę powołania ABI,

4) oświadczenie ABI o pełnej zdolności do czynności prawnych, posiadaniu odpowiedniej wiedzy w zakresie ochrony danych osobowych i niekaralności za umyśle przestępstwo

GIODO może wydać decyzję o wykreśleniu ABI z rejestru, jeżeli okaże się, że:

- ABI nie spełnia warunków wskazanych w oświadczeniu (lub jego zastępcy nie spełniają tych warunków);
- ABI nie prowadzi rejestru zbiorów,
- Administrator danych nie zgłosił do GIODO informacji o odwołaniu ABI.

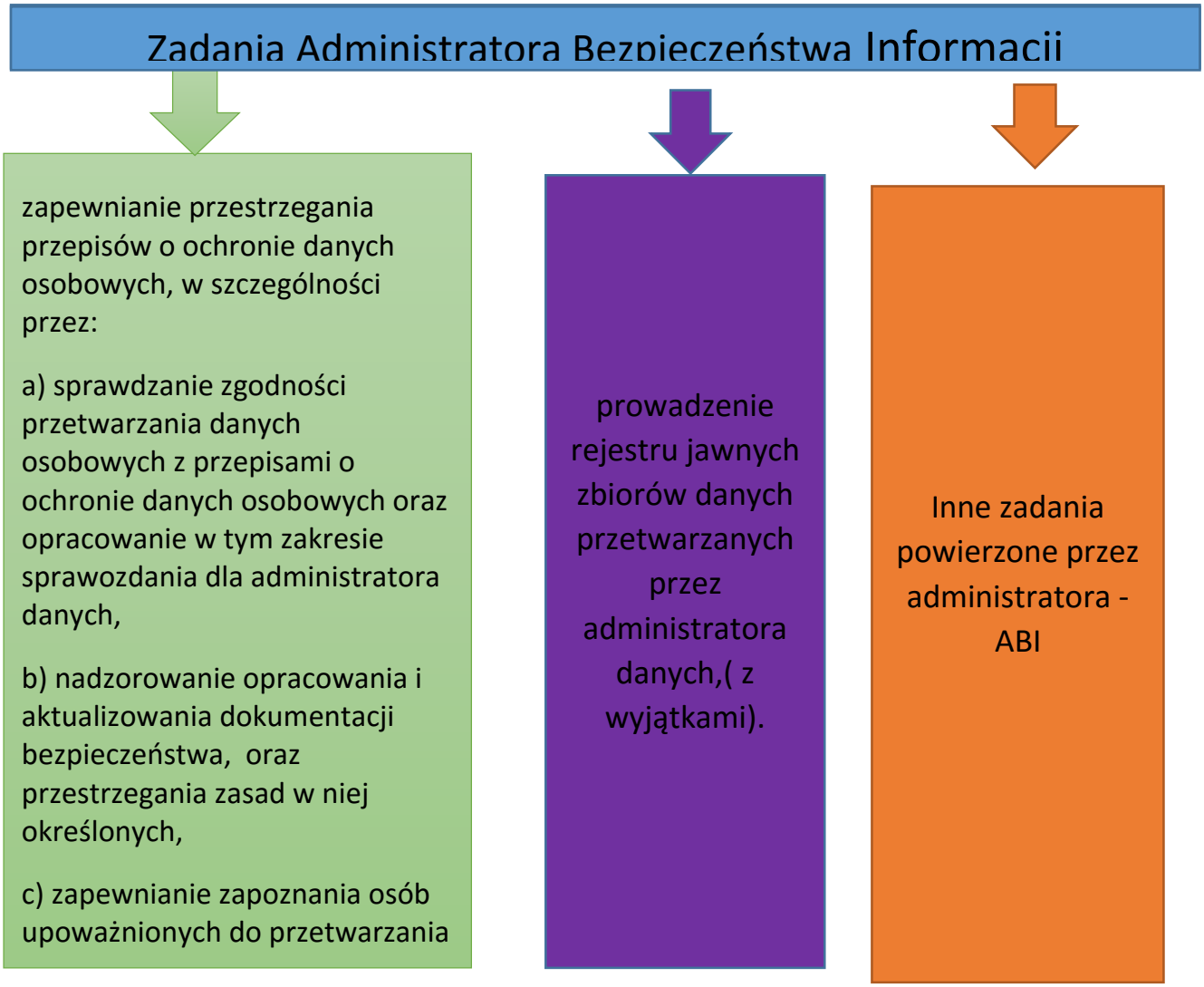
Odwołanie ABI powinno zostać zgłoszone do rejestru także w terminie 30 dni od zaistnienia okoliczności powodujących odwołanie. ABI powinien zostać odwołany ze stanowiska w przypadku, gdy przestał spełniać wymogi: niekaralności, czy został pozbawiony praw publicznych.

[5] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji Dz.U. 2014 poz. 1934

Tytuł „Administratora Bezpieczeństwa Informacji" zastrzeżony jest jedynie dla ABI zgłoszonych do rejestracji. Osoba zajmująca się zatem „w okresie przejściowym" ochroną danych osobowych, która nie zostanie zgłoszona do rejestru GIODO, nie powinna być tytułowana jako ABI ale np. jako specjalista ds. ochrony danych osobowych[6].

Zadania ABI

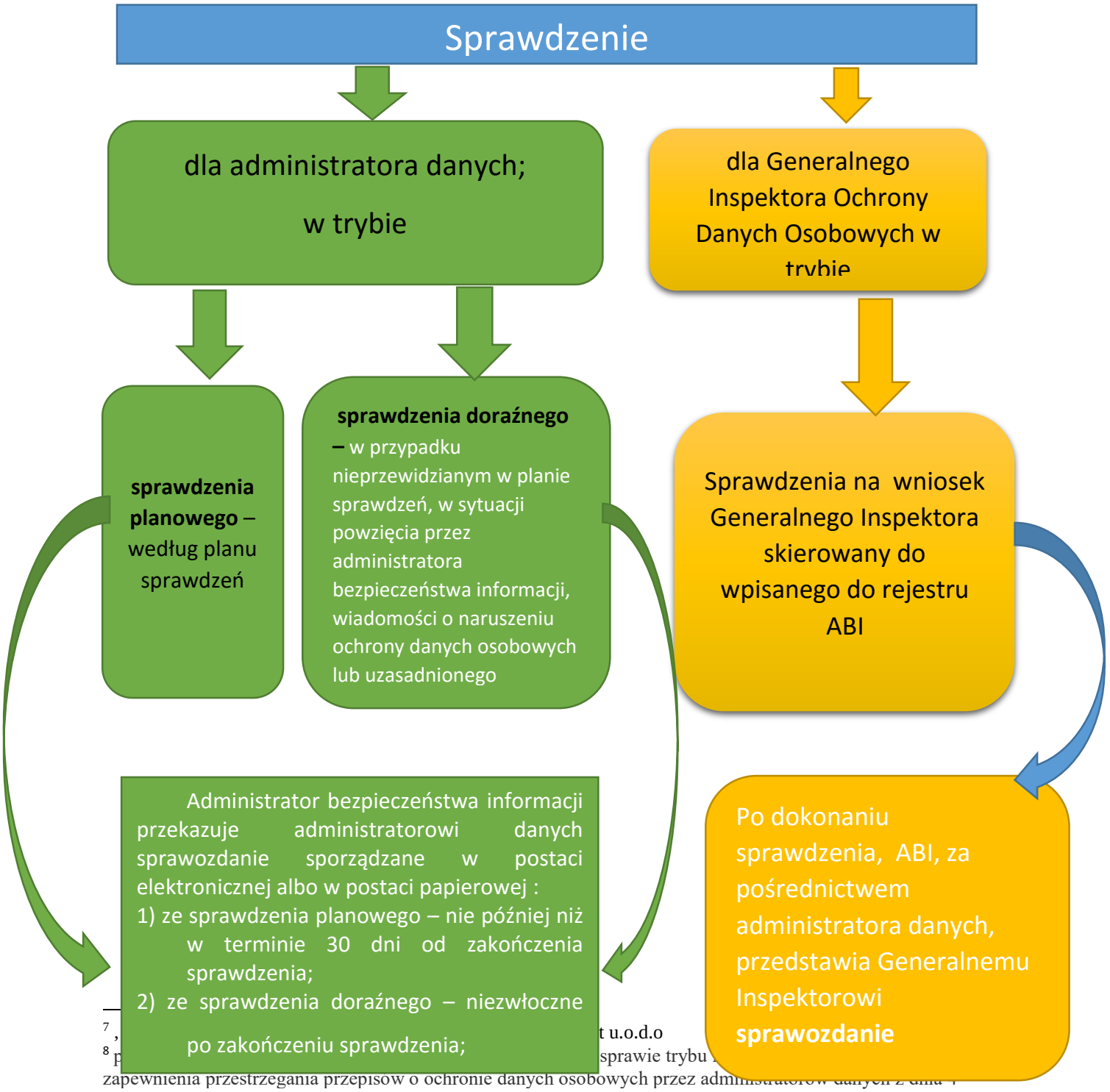
Do zadań Administratora Bezpieczeństwa Informacji należą przede wszystkim zadania przedstawione na rysunku 1:



[6] CO Z TYM ABI? T.Osiej, M Bargiel –portal e-ochrona.danych.pl http://www.e-ochronadanych.pl/artykuly.php?news_id=2426

Rysunek 1. Zadania Administratora Bezpieczeństwa Informacji. Opracowanie własne

Niezwykle ważne zadnie wiąże się z procedurą sprawdzenia[7], Sprawdzenie to czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych[8,](Rysunek 2)



[7], t u.o.d.o

[8] p sprawie trybu ... zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratorów danych z dnia 4 marca 2015 r. http://legislacja.rcl.gov.pl/projekt/268582/katalog/268589#268589

Rysunek 2. Schemat różnych wariantów przeprowadzania przez ABI procedury sprawdzenia.

Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności:

- zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz
- konieczność weryfikacji zgodności przetwarzania danych osobowych z zasadami i wymaganiami wynikającymi z ustawy.

Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan jest przedstawiany administratorowi danych nie później niż na miesiąc przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na dwa lata.

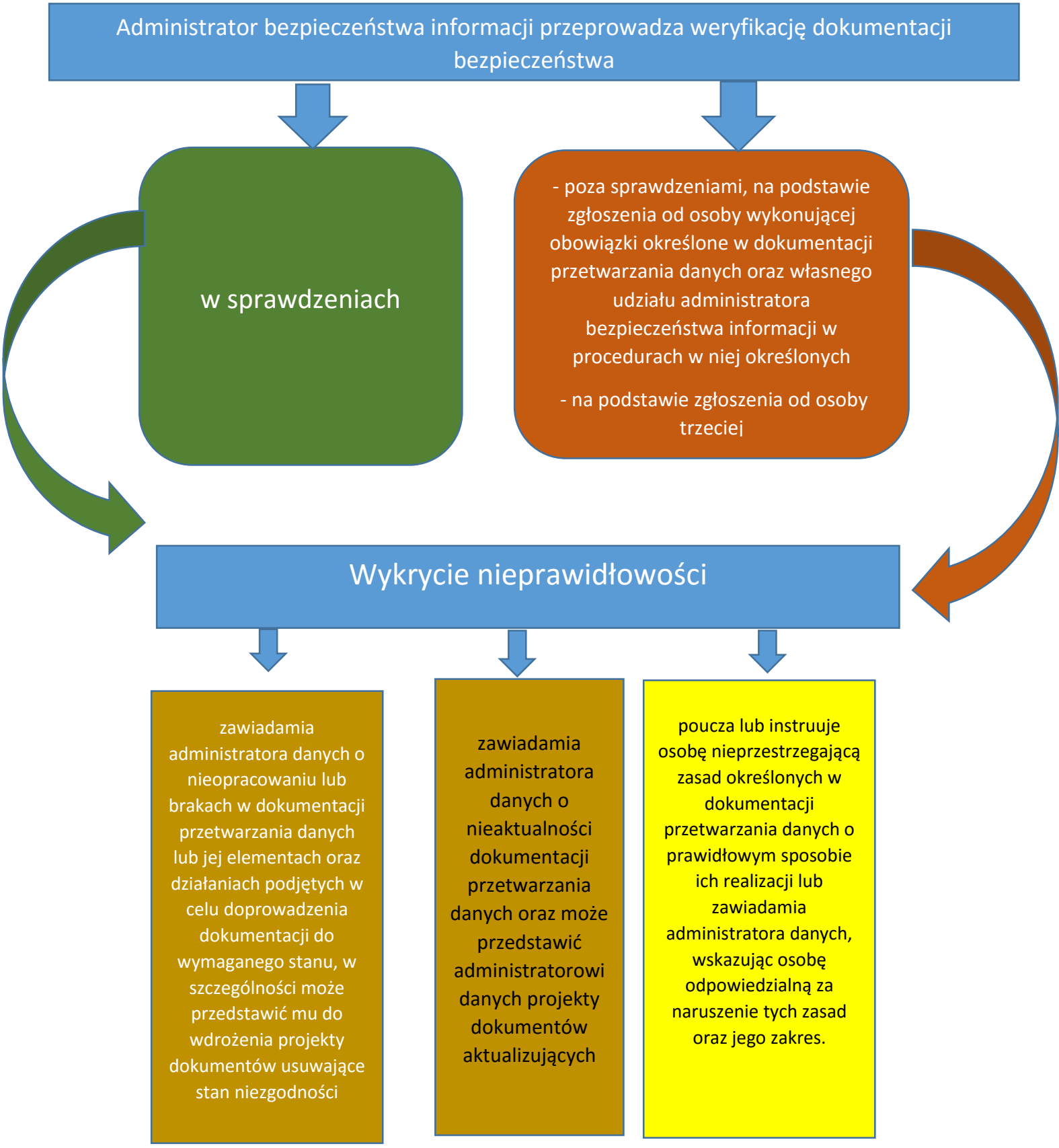
Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu przez administratora bezpieczeństwa informacji, wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego przed podjęciem pierwszej czynności w toku sprawdzenia. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie.

Wśród zadań administratora bezpieczeństwa informacji jednym z najważniejszych jest nadzór nad dokumentacją przetwarzania danych (Tabela 1). Sprawując nadzór nad dokumentacją przetwarzania danych administrator bezpieczeństwa informacji dokonuje weryfikacji dokumentacji bezpieczeństwa oraz podejmuje działania w przypadkach wykrycia nieprawidłowości (Rysunek 3).

Zadania ABI w zakresie nadzoru nad dokumentacją bezpieczeństwa
1) weryfikacja kompletności dokumentacji przetwarzania danych;
2) ocena zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
3) analiza stanu faktycznego w zakresie przetwarzania danych osobowych;
4) ocena zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych
5) ocena przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania

danych

Tabela nr 1 - Zadania ABI w zakresie nadzoru nad dokumentacją bezpieczeństwa, opracowanie własne na podstawie projektu rozporządzenia Ministra Administracji i Cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (z dn. 10.04.2015)



Rysunek 3. Nadzór nad dokumentacją przetwarzania danych realizowany przez ABI. Opracowanie własne na podstawie Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji

Zgłaszanie zbiorów danych osobowych czy rejestr zbiorów danych

Uwzględniając sygnały z prac nad regulacjami UE wprowadzono pewne złagodzenia dotyczące zgłaszania zbiorów danych osobowych do Generalnego Inspektora Danych Osobowych. Wprowadzono zasadę, że jeżeli w podmiocie przetwarzającym dane osobowe zostanie powołany administrator bezpieczeństwa informacji wszystkie zbiory danych osobowych (zwykłych) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych tzn. znajdujące się na nośnikach papierowych zostają zwolnione z obowiązku rejestracyjnego[9].

Natomiast z obowiązku rejestracji zbiorów danych osobowych zwykłych również tych przetwarzanych z wykorzystaniem systemów informatycznych, zwolnieni zostali administratorzy danych, który powołali administratora bezpieczeństwa informacji i zgłosili go Generalnemu Inspektorowi do rejestracji.[10]

Bez zmian pozostaje natomiast obowiązek rejestrowania danych wrażliwych i prawo do przetwarzania ich zbiorów dopiero po otrzymaniu decyzji o zarejestrowaniu.

Obowiązek rejestracji zbiorów zastąpiono obowiązkiem prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych[11]. Rejestr zbiorów danych

[9] Art. 43 ust.1 pkt.12 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883

[10] Art. 43 ust.1a Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883

[11] Stowarzyszeni Administratorów Bezpieczeństwa Informacji **KALENDARIUM NOWELIZACJI USTAWY O OCHRONIE DANYCH OSOBOWYCH - USTAWA DEREGULACYJNA**
http://www.sabi.org.pl/page8.php

składa się z wykazu zbiorów danych zawierającego odrębnie dla każdego zbioru danych informacje. Rejestr prowadzony jest w postaci papierowej lub w postaci elektronicznej.

W przypadku prowadzenia rejestru w postaci elektronicznej, administrator bezpieczeństwa informacji udostępnia do przeglądania rejestr:

- na stronie internetowej administratora danych, przy czym na stronie głównej umieszcza się odwołanie umożliwiające bezpośredni dostęp do rejestru, lub
- na stanowisku dostępowym w systemie informatycznym administratora danych znajdującym się w siedzibie lub miejscu zamieszkania tego administratora, lub
- przez sporządzenie wydruku rejestru z systemu informatycznego administratora danych.

W przypadku prowadzenia rejestru w postaci papierowej, administrator bezpieczeństwa informacji udostępnia do przeglądania każdemu zainteresowanemu treść rejestru w siedzibie lub miejscu zamieszkania administratora danych.

Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru:

1) przed rozpoczęciem przetwarzania w zbiorze danych wpisuje zbiór danych do rejestru;
2) aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem;
3) wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych;
4) udostępnia rejestr do przeglądania.

Wszystkie wyżej wymienione obowiązki administratora danych i ABI mają spowodować lepsza ochronę danych i skuteczne zapobieganie ich naruszeniom. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób; głęboko zaszyfrowane dane, w przypadku których istnieją dowody na to, że kod szyfrujący nie został złamany, nie są objęte tymi przepisami.

Naruszenie ochrony danych osobowych, w braku odpowiedniej i szybkiej reakcji, może prowadzić do znacznej straty ekonomicznej i szkód społecznych u danej osoby, w tym oszustwa dotyczącego tożsamości. Z tego względu administrator danych powinien zawiadomić organ nadzorczy o naruszeniu niezwłocznie, przy czym zakłada się, że oznacz to

nie później niż po72 godzinach. W stosownym przypadku do zawiadomienia należy dołączyć stosowne wyjaśnienie powodów opóźnienia. Osoby, których dane osobowe mogłyby ucierpieć wskutek takiego naruszenia, powinny być niezwłocznie zawiadamiane, aby umożliwić im podjęcie niezbędnych środków ostrożności. Naruszenie powinno być uznawane za wywierające niekorzystny wpływ na dane osobowe lub prywatność podmiotu danych, jeżeli jego skutkiem mogą być np. kradzież lub oszustwo dotyczące tożsamości, uszkodzenie ciała, poważne upokorzenie lub naruszenie dobrego imienia. Zawiadomienie powinno zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla osoby zainteresowanej dotyczące ograniczenia potencjalnych niekorzystnych skutków naruszenia. Zawiadomienia powinny być przekazywane podmiotom danych tak szybko jak to racjonalnie możliwe, w ścisłej współpracy z organem nadzorczym oraz z poszanowaniem wytycznych przekazanych przez ten organ lub inne właściwe organy (np. organy ścigania). Na przykład szansa ograniczenia przez podmioty danych bezpośredniego ryzyka szkody wymagałaby szybkiego zawiadomienia podmiotów danych, zaś potrzeba wdrożenia właściwych środków w przypadku powtarzających się lub podobnych naruszeń ochrony danych może usprawiedliwiać dłuższe opóźnienie[12].

Literatura

1. T. Osiej M. Bargiel CO Z TYM ABI? http://www.e-ochronadanych.pl/artykuly.php?news_id=2426
2. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji Dz.U. 2014 poz. 1934
3. KALENDARIUM NOWELIZACJI USTAWY O OCHRONIE DANYCH OSOBOWYCH - USTAWA DEREGULACYJNA http://www.sabi.org.pl/page8.php
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji Dz.U. 2015 poz. 745
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji Dz.U. 2014 poz. 1934
6. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych Dz.U. 2015 poz. 719
7. Ł. Onysyk Jak prowadzić rejestr zbiorów danych osobowych http://blog.e-odo.pl/2015/01/13/jak-prowadzic-rejestr-zbiorow-danych-osobowych/

[12] 67

8. P.Janiszewski Projekt rozporządzenia w sprawie realizacji zadań przez ABI http://blog.e-odo.pl/2015/01/05/projekt-rozporzadzenia-w-sprawie-realizacji-zadan-przez-abi/
9. K.Chylińska Nowe rozporządzenie w sprawie abi http://blog.e-odo.pl/author/katarzyna-chylinska/
10. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
11. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/
12. K. Witkowska Ochrona danych osobowych 2015 – zmiana przepisów, nowe obowiązki i nowe korzyści. http://ksiegowosc.infor.pl/obrot-gospodarczy/dzialalnosc-gospodarcza/703554,Ochrona-danych-osobowych-2015-zmiana-przepisow-nowe-obowiazk

Streszczenie

Analizując wprowadzone w Polsce przepisy ustawy, a także planowane na 2016 rok regulacje UE dotyczące przetwarzania danych osobowych w UE wydaje się, że w przypadku podmiotów leczniczych i systemu informacyjnego opieki zdrowotnej w większości przypadków koniecznym będzie powołanie Administratora Bezpieczeństwa Informacji (ABI). W artykule przedstawiamy najważniejsze aspekty funkcjonowania ABI, wymagania stawiane przed ABI, konieczność rejestracji i obowiązki. Warunkiem koniecznym prawidłowego usytuowania w podmiocie leczniczym , jest zgłoszenie powołanego ABI w terminie 30 dni od powołania do rejestru prowadzonego przez GIODO. Najważniejszymi zadaniami ABI są zapewnianie przestrzegania przepisów o ochronie danych osobowych, w tym, prowadzenie rejestru zbiorów danych osobowych, dokonywanie sprawdzeń oraz nadzór nad dokumentacją przetwarzania danych.